STATEMENT OF THE HONORABLE KAREN EVANS ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY OFFICE OF MANAGEMENT AND BUDGET BEFORE THE COMMITTEE ON GOVERNMENT REFORM U.S. HOUSE OF REPRESENTATIVES

June 29, 2005

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to speak about the Federal government's efforts in preparing for the transition to Internet Protocol version 6 (IPv6).

This morning I would like to briefly discuss some benefits of IPv6, highlight some challenges in making the transition, and identify the steps we are taking to address those challenges.

The transition to IPv6 is more than an upgrade of the existing protocol. IPv6 is replete with new features and functions such as expanded address space, improved flexibility and functionality, improved information routing, enhanced mobility features, simplified activation, configuration and operation of networks and services, and once fully implemented, improved security. IPv6 when fully functional will ultimately result in a number of benefits, but more importantly a new communication paradigm.

Some benefits of IPv6 will be directly to logistics and consumers. IPv6, combined with Radio Frequency Identification Tags and integrated into mobile phones and consumer electronics, will support new ways of thinking about the way business is conducted and the way consumers could buy goods and services. Other benefits of IPv6 will be directly to commuters and first responders. For example, IPv6 combined with Dedicated Short-Range Communication technology, could lead to smarter and safer cars, fewer traffic delays, and an improved ability for first responders to signal drivers of their rapid approach while controlling the stop lights at an intersection.

Actually, the paradigm shift has already started in the Federal government because IPv6 capable software and hardware already exist in Federal government networks (and elsewhere). Most current computer operating systems support IPv6 and many installed base of routers and switches already have IPv6 built-in. In other words, the transition to IPv6 is already taking place, but it has many challenges -- including planning for system migration, security aspects of the transition, and as yet undefined privacy concerns of the technology itself.

As I mentioned in my April 7, 2005, testimony before this committee regarding our efforts to safeguard the government's information and systems, late last fall OMB directed the agencies to provide a preliminary report on their planning activities for the transition to IPv6. Only the Department of Defense had undertaken any significant effort in this area. Given the lack of government-wide progress and our concern regarding the complexities of transition, we recognized the need to begin developing a comprehensive transition planning guide and process.

We are about to take the first step and issue a policy memorandum providing guidance to the agencies to ensure an orderly and secure transition to IPv6. The purpose of the guidance will be to ensure effective planning and to raise the level of awareness and urgency of preparing for IPv6. Later in my testimony I will discuss the key elements of the policy.

As you know, the Government Accountability Office (GAO) recently released a report identifying a number of significant IPv6 challenges. A draft report, published for public notice and comment by the Department of Commerce, also identifies many of the same challenges. Both reports describe careful planning as a key for Federal agencies to make an orderly transition and both emphasize the need to ensure the security of agency information and networks during the transition.

On the security issue, and to underscore the complexity of planning for the transition, not all experts agree on the extent of the security risk involved in the IPv6 transition. The most telling example of these differing views comes from experts developing today's most commonly used computer operating system. They have expressed skepticism regarding the level of risk highlighted in the GAO report. We continue to discuss this issue with them at staff and senior levels and are awaiting their comments on the GAO report and will provide those comments to GAO as well.

The overarching challenge facing us is ensuring continued uninterrupted functionality of Federal agencies during the transition while providing continued and improved information assurance. This will require major changes in the architecture of many agency networks. Since there is a large embedded base of IPv4-compatible equipment and applications, transitioning to IPv6 will also require large capital investments and labor resources. While the challenges are significant, they are not insurmountable, especially if we approach them methodically and in phases.

Let me begin by sharing with you what we are doing to address these challenges.

As I mentioned earlier, we are about to issue a policy memorandum providing guidance to the agencies to ensure an orderly and secure transition to IPv6. The guidance will lay out five important actions the agencies should take.

First, agencies will have to familiarize themselves to the transitions issues by reviewing the GAO report, Commerce report, and particularly the Department of Homeland Security's US-CERT advisory of security issues concerning IPv6. Since IPv6 is already present in many Federal networks, it is important that agencies begin addressing the security risks associated with IPv6 now.

Second, agencies will have to assign a specific individual to lead and coordinate agency planning. This person will be responsible for monitoring, enforcing, and reporting on the transition and implementation of IPv6 within the agency.

Third, agencies will develop an inventory of existing IP capable devices and technologies. To ensure an orderly transition from IPv4 to IPv6, we must establish a baseline and determine the size of the problem. While we know IPv6 technologies are deployed throughout the government, but like other organizations, we do not know specifically which ones, how many there are, or precisely where they are located. We are planning for each agency to file a report of their inventory of IP capable devices and technologies to OMB in the first quarter of FY 2006.

Fourth, agencies will conduct an impact analysis to determine fiscal and operational impacts and risks during the transition to IPv6. We are planning for each agency to report the results of this impact analysis to OMB in the first quarter of FY 2006, and it should include analysis on cost and risk. For cost, the agencies must report on estimates for planning, infrastructure acquisition (above and beyond normal expenditures), training, and risk mitigation.

As for all other planning for investments in information technology, agencies' IPv6 analyses will include a risk inventory and assessment using the criteria set forth in existing OMB capital planning and investment control policy found in OMB Circular A-11, Section 300. This policy requires agencies to discuss a range of risks and present a plan to eliminate, mitigate, or manage them, with milestones and completion dates. Assessments will include areas such as life-cycle costs, schedules, reliability of systems, dependencies and interoperability between systems, asset and information protection, and information privacy.

Fifth, the policy will direct the CIO Council to develop before the end of the calendar year, more detailed IPv6 implementing guidance. It will include guidance for developing detailed prioritized schedules and milestones (e.g., a sequencing plan), integrating IPv6 with the agency enterprise architecture, developing necessary IPv6-related policies and compliance mechanisms, training material, and test plans for IPv6 compatibility and interoperability. To the extent the agencies are currently capable of addressing the elements of the future CIO Council guidance, they have been instructed to begin doing so now.

Developing detailed prioritized schedules and milestones is especially important for integrating agency IPv6 transition activities with their enterprise architectures and thus ensure the transition is consistent with and supporting of their mission and business needs. We will use the OMB EA Assessment Framework to measure the degree to which agencies are effectively performing this planning element.

Our policy will also set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure. Once the network backbones are ready, the applications and other elements will follow. Setting this firm date is necessary to maintain focus on this important issue. Overall the actions set out in our policy will begin to address the many challenges that come with IPv6 transition.

We are also now discussing with the National Institute for Standards and Technology whether we need a Federal Information Processing Standard for IPv6 and are preparing an amendment to the Federal Acquisition Regulation to include language on IPv6.

Conclusion

Thank you for this opportunity to discuss the Administration's strategy on IPv6. As we continue to work with the agencies to move toward an IPv6 environment, we will continue to look for new opportunities to refine our oversight of this important initiative. We appreciate your interest in OMB's role in IPv6 and will continue our efforts to drive improved performance and results throughout the Executive branch agencies.

Thank you. I will be happy to answer any questions at this time.